

Webszerver készítés alapjai: NGINX

1. *sudo -s*

2. *apt-get install nginx-full*

3. config file teszt

1. *nginx -t*

4. alap beállítások

1. *vi /etc/nginx/nginx.conf*

1. events részbe:

1. use epoll;

1. <http://wiki.nginx.org/NginxOptimizations>

2. max clients = worker_processes × worker_connections

1. fő részbe:

1. worker_processes 4;

1. célszerűen a CPU-k illetve CPU magok száma

2. sok statikus fájl esetén érdemes növelni

3. egyes worker processzek CPU-hoz kötése:

1. worker_processes 4;

2. worker_cpu_affinity 0001 0010 0100 1000;

2. events részbe:

1. worker_connections 768;

3. limitáld a max. megnyitható fájlokat workerenként:

1. fő részbe:

1. worker_rlimit_nofile 4096; (core)

1. /etc/default/nginx

1. ULIMIT="-n 4096"

2. /etc/security/limits.conf !!!

4. gzip használata (HTTP szekció)

1. csökkenti az átvitt adatmennyiséget, így a hálózati terhelést

2. nem minden kliens kezeli jól (pl. msie6 nem)

3. gyári konfigurációk jók, plusz

1. gzip_min_length 10240;

2. gzip_proxied expired no-cache no-store private auth;

1. a proxytól jövő kérések tömörítésének engedélyezése/tiltása

2. a "via" fejléc alapján érzékeli, hogy proxytól jön-e a kérés

5. extrém sebesség növelés

1. Linux kernel opciók

1. *scp sysctl-local.conf server:*

2. *cat sysctl-local.conf*

3. *mv sysctl-local.conf /etc/sysctl.d/local.conf*

4. *start procps*

2. sendfile on; (HTTP szekció)

1. lényegesen gyorsabb, mint a read/write syscall

3. tcp_nopush=on; (HTTP szekció)

1. sendfile on kell hozzá

2. TCP_CORK opció használata: egy csomagban igyekszik elküldeni az összes http response fejléceket

4. multi_accept on; (events szekció)

1. gyorsabban fogadja a kapcsolatokat, de túltöltheti a worker_connectiont, ha az túl kicsi
5. keepalive_timeout csökkentése (HTTP szekció)
6. reset_timedout_connection on; (HTTP szekció)
 1. TCP RST-vel zárja le a kapcsolatokat, így elmarad a sok FIN_WAIT1
7. client_header_timeout és client_body_timeout csökkentése (alap: 60s, HTTP szekció)
 1. csak akkor hat, ha a fejléct és a törzset külön küldi a kliens
 2. megakadályozza, hogy a kliens feltartsa a szerveret lassú kéréssel
8. send_timeout drasztikus csökkentése (alap: 60s)
 1. az egyes read műveletekre vonatkozik, NEM a teljes oldalra: azaz ha a kliens ennyi ideig nem olvas adatot, a kapcsolat lezárásra kerül (de ha sok az adat és folyamatos az olvasás NEM hat)
9. open_file_cache
 1. open_file_cache max=100000 inactive=20s;
 2. open_file_cache_valid 30s;
 3. open_file_cache_min_uses 2;
 4. open_file_cache_errors on;

10.nginx -t

6. https

1. SSL kulcs https-hez
 1. *apt-get install gnutls-bin*
 2. certtol használata
 1. *cd /etc/nginx*
 2. kulcs készítése: *certtool --sec-param high -p --outfile https.key*
 3. aláírás kérelem elkészítése hivatalos hitelesítéshez (vagy saját CA-hoz)
 1. *certtool -q --load-privkey https.key --outfile https.csr*
 2. *cat https.csr*
 3. a csr fájlt kell beküldeni a hitelesítő szervhez
 4. magadnak saját magával (self signed)
 1. *certtool -s --load-privkey https.key --outfile https.crt*
 5. meglévő tanúsítvány adatainak megnézése
 1. *certtool -i --infile https.crt*
 2. *ls -lh https.**
2. https beállítása
 1. *scp ssl.conf server:*
 2. *cat ssl.conf*
 3. *mv ssl.conf /etc/nginx/conf.d/*
 4. *nginx -t*
 5. *service nginx restart*
 6. és kell egy https-en kiszolgáló virtualhost

7. virtuális szerverek

1. webszerver http
 1. böngészőben: <http://linuxakademia.lan>
 1. nginx alap jön be rá
 2. *mkdir -p /srv/web/linuxakademia*
 3. *date > /srv/web/linuxakademia/date.txt*
 4. *scp linuxakademia server:*

5. `cat linuxakademia`
6. `mv linuxakademia /etc/nginx/sites-available/`
7. `ln -s /etc/nginx/sites-available/linuxakademia /etc/nginx/sites-enabled/`
8. `nginx -t`
9. `service nginx restart`
10. böngészőben: <http://www.linuxakademia.lan>
 1. forbidden
 2. `tail /var/log/nginx/linuxakademia_error.log`
 3. <http://www.linuxakademia.lan/date.txt>
 1. működik
2. webszerver https
 1. `scp linuxakademia-ssl server:`
 2. `cat linuxakademia-ssl`
 3. `mv linuxakademia-ssl /etc/nginx/sites-available/`
 4. `ln -s /etc/nginx/sites-available/linuxakademia-ssl /etc/nginx/sites-enabled/`
 5. `nginx -t`
 6. `service nginx restart`
 7. böngészőben: <https://www.linuxakademia.lan/date.txt>

8. naplózás

1. virtuális szerverenként célszerű
2. `access_log`
 1. `log_format`
 1. `scp log.conf server:`
 2. `cat log.conf`
 3. `mv log.conf /etc/nginx/conf.d/`
 4. `vi /etc/nginx/sites-available/linuxakademia`
 1. `access_log /var/log/nginx/linuxakademia_access.log myformat;`
 5. `tail /var/log/nginx/linuxakademia_access.log`
 1. Ez az alapértelmezett, lehet bővíteni.
 2. http://wiki.nginx.org/HttpLogModule#log_format
 2. több log: több `access_log` bejegyzés
 3. GEO IP
 1. `sudo apt-get install geoip-database`
 2. `wget`

<http://geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz>
 3. `gunzip GeoLiteCity.dat.gz`
 4. `mv GeoLiteCity.dat /usr/share/GeoIP/`
 5. `scp geoip.conf server:`
 6. `cat geoip.conf`
 7. `mv geoip.conf /etc/nginx/conf.d/`
 8. `vi /etc/nginx/sites-available/linuxakademia`
 1. `access_log /var/log/nginx/linuxakademia_access.log geoiplog;`
 9. `nginx -t`
 10. `service nginx reload`
 11. Böngészőben: <http://www.linuxakademia.lan/date.txt>
 12. `tail /var/log/nginx/linuxakademia_access.log`
 13. A teszthez verjük át a rendszert:
 1. `iptables -t nat -I INPUT -s 192.168.200.10 -p tcp --dport 80 -j SNAT`

--to-source 212.52.168.10

14.böngészőben: <http://www.linuxakademia.lan/date.txt>

15.tail /var/log/nginx/linuxakademia_access.log

9. Korlátozások

1. Egyszerű limit

1. *vi /etc/nginx/sites-available/linuxakademia*

1. lásd location részt kommentezve!

2. GEO IP

1. *vi /etc/nginx/conf.d/geoip.conf*

1. *map \$geoip_country_code \$allowed_country {*

2. *default no;*

3. *HU yes;*

4. *}*

2. *vi /etc/nginx/sites-available/linuxakademia*

1. *if (\$allowed_country = no) {*

2. *return 444;*

3. *}*

3. *nginx -t*

4. *service nginx reload*

5. böngészésben:

1. <http://www.linuxakademia.lan/date.txt>

1. megy

2. Szüntessük meg az átverést!

1. *iptables -t nat -D INPUT -s 192.168.200.10 -p tcp --dport 80 -j SNAT --to-source 212.52.168.10*

3. <http://www.linuxakademia.lan/date.txt>

1. nem megy

2. *tail /var/log/nginx/linuxakademia_access.log*

3. Kérések száma / idő, kliensenként

1. *scp limit.conf server:*

2. *cat limit.conf*

3. *mv limit.conf /etc/nginx/conf.d/*

4. *nginx -t*

5. *service nginx reload*